(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
18 July 2002 (18.07.2002)

PCT

(10) International Publication Number
WO 02/056536 A1

(51) International Patent Classification[7]: H04L 9/06

(21) International Application Number: PCT/NL01/00008

(22) International Filing Date: 9 January 2001 (09.01.2001)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: **TELEFONAKTIEBOLAGET LM ERICSSON** [SE/SE]; Telefonvagen 30, S-126 25 Stockholm (SE).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **WEINANS, Erwin** [NL/NL]; Vechtvoorde 96, NL-7772 VC Hardenberg (NL).

(74) Agent: **VAN DER AREND, A., G., A.**; Exter Polak & Charlouis B.V., P.O. Box 3241, NL-2280 GE Rijswijk (NL).

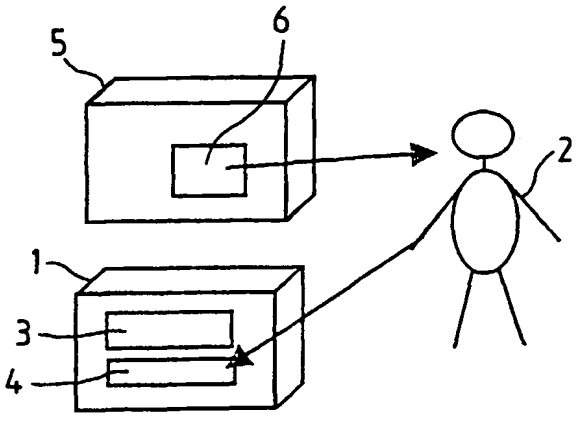
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHOD AND SYSTEM FOR BONDING TWO BLUETOOTH DEVICES



(57) Abstract: Method and system for bonding a first Bluetooth device (5, 8) to a second Bluetooth device (1, 15, 22), with both devices placed in a bonding mode, by having the first devcie to generate a random passkey and transmitting it in a manner which is descernible by a user (2) of the devices, or by sensor means (11, 19) of a reader unit (10, 18), or by sensor means (23) of the other device (22). The reader unit (10) may convert a received signal carrying a passkey which is undiscernible by the user (2) into a presentation which is discernible by user (2). Upon discerning the password the user (2) may enter the password in the other device (1) in the usual way. Said other Bluetooth device (15, 22) may have sensor means (16, 23) for sensing a signal carrying a password transmitted by a reader unit (18) or by the Bluetooth device (8).

WO 02/056536 A1

Title: Method for bonding two Bluetooth devices and system suitable for applying the method.

The invention relates to a method for bonding two Bluetooth devices as described in the preamble of claim 1. The invention also relates to a system which is suitable for applying the method as described in the preamble of claim 6.

The Bluetooth technology provides for a short range connection between devices based on 2.4 GHz radio technology. The range is about 10 meters and the devices do not have to be in line of sight to communicate. The maximum bandwidth for data traffic is 1 Mb per second. Bluetooth is operating in the free ISM band, which is also used by many other devices. Bluetooth prevents disturbance by other devices by hopping over 79 frequencies every 1/1600 second.

When a communication cable between two devices is replaced by the use of radio signals for communication there will be a need to prevent eavesdropping and falsifying transmitted messages. Therefore the Bluetooth technology has built-in functionality for authentication and encryption. Authentication is used to prevent unwanted access to data and to prevent falsifying of message originator. Encryption is used to prevent eavesdropping. These two techniques combined with the frequency hopping technique and the limited transmission range for a Bluetooth unit give the technology higher protection against eavesdropping. Dependent on the application which is to be executed the Bluetooth concept provides three levels of security:

1. non-secure; this mode bypasses functionality for authentication and encryption.

2. service-level security; security procedures on this level have not been fully established yet.

3. link-level security; security procedures are initiated before the link set-up upon completion of a Link Manager Protocol (LMP) which is responsible for link set-up between Bluetooth devices.

The link-level security mode is based on the concept of link keys. These keys are secret 128 bit random numbers stored individually for each pair of devices in a Bluetooth connection. Each time two Bluetooth devices communicate the link key is used for authentication and encryption. Both devices contain the same link key which is generated locally in each device based on a passkey which is common for both devices or common information derived from such passkey. The link key is kept secret in each device.

If one wants to use two Bluetooth devices with secure communication between the devices it is necessary to firstly create a trusted relationship between the devices by the user. To that end the user puts the devices in a bonding mode upon which the devices ask the user to enter a passkey, which may be selected arbitrarily by the user. Upon entering the passkey in a device the device will generate a piece of information based on the passkey. The piece of information will be identical for both devices. From then on the two devices are bonded and there is no need to keep the passkey by the user or the devices any longer. In a second stage the passkey based piece of information is used by each device to generate and store a common link key. From that moment on the two devices are paired. The next time the devices get connected the stored link key on both sides will be checked. If the link keys match no request for entering a passkey will be generated. If the link keys do not match the above bonding and pairing procedures must be carried out again.

If the Bluetooth devices which are to be bonded are both equipped with display means and manual input means, in particular a keyboard, there will be no difficulty to enter the passkey by a user of the devices for the bonding procedure.

If one device is not equipped with such an input device the device presently needs to contain a factory programmed passkey. There are two common ways of handling stored passkeys. Firstly the passkeys may be default identical for all manufactured devices of a specific type. Secondly the passkeys may be unique per device.

A drawback of the first solution of handling a factory programmed passkey is that the Bluetooth security is weakened. Since the value of the passkey is essential for creating the link key and the passkey being identical for all devices of the same type a Bluetooth connection between them cannot be considered secure.

A drawback of the second solution is that the manufacturer must maintain a logistic system for handling the many different passkeys, each unique passkey must be communicated to its ultimate user individually, e.g. printed on a box containing a specific Bluetooth device in which the passkey is stored, and the manufacturer must provide a way to restore devices for which the passkey is lost. There must be a support organisation for handling lost passkey requests. Such a logistic and supporting system will be very complex and expensive to maintain.

It is an object of the invention to solve the above mentioned drawbacks.

Therefore the invention provides a method as described in claim 1.

With the method according to claim 1, for entering a passkey in a Bluetooth device, the device needs not to be equipped with a keyboard or such type of physical interface, but any other non-radio communication interface can be used. In particular such non-radio communication interface is part of the device in the first place for normal use of the device. The device may present the randomly generated passkey in several ways, such as by transmission of sound or light.

When applying the method according to the invention the manufacturer may make all Bluetooth devices generic. Still, the devices are able to support Bluetooth encryption in a secure way. There are no logistical costs attached to the method. Since the passkey is uniquely generated every time the device needs to be bonded with another device and on demand by a user of the devices, loosing a passkey is not longer an issue and therefore does not impose costs for retrieving same.

The above mentioned drawbacks are solved also by a system as described in claim 6.

The invention will be described in further detail with reference to the accompanied drawings in which:

fig. 1 shows schematically a system in which a prior art method is applied for entering a passkey into two Bluetooth devices by a user thereof;

figs. 2, 3, 4 and 5 show first to fourth examples respectively of a system according to the invention in which the method according

to the invention for entering a passkey into two Bluetooth devices is applied.

The prior art method shown schematically in fig. 1 is suitably for manually entering a passkey into two Bluetooth devices 1 by a user 2. The devices 1 may comprise a display means 3 and an input means 4, such as a keypad.

The arrows shown in fig. 1-5 indicate the entering or transmission of a passkey.

Although indicated as Bluetooth devices, the devices 1 and those to mention may in fact be larger or complexer pieces of equipment containing a pure Bluetooth device integrated therewith. For simplicity the devices as a whole are called Bluetooth device.

The user 2 may choose any suitable passkey arbitrarily. Upon putting the devices 1 in a bonding mode the user 2 may enter the passkey into both devices 1 by using their input means 4. Upon completion thereof each device 1 will use the passkey to generate a link key which will be identical for both devices 1. With every communication session between the devices 1 the devices 1 will check the identity of their link keys by transmitting data which is encrypted by the link key and by analysing a similar received transmission for its validity or identity with the locally stored link key.

The method exemplified by fig. 2 may be applied for providing a common passkey to two Bluetooth devices, such as devices 1, 5, of which one device 5 does not comprise the input means 4 and possibly not the display means 3 of the device 1. Instead, device 5 is provided with some kind of transmission means 6. The transmission means 6 may be an acoustic or optical transducer for transmitting a sound signal or light signal respectively which is discernible by the user 2. The light signal may be of any type, such as light flashes or the display of readable characters.

Bluetooth device 5 contains a random number generator (not shown) for generating a random passkey upon putting the device 5 in bonding mode by user 2. Device 5 will transmit the randomly generated passkey, such that the user 2 can hear, read or otherwise discern the passkey. Then, user 2 may enter the passkey discerned from device 5 into the other device 1 in the same way as with the prior art method shown in fig. 1.

Preferably the transmission means 6 of device 5 consist of means which are incorporated in device 5 anyway for normal use of device 5, that is apart from said bonding.

The method exemplified by fig. 3 differs from the method shown by fig. 2 in that Bluetooth device 5 is replaced by Bluetooth device 8 having transmission means 9, and comprising in addition a reader unit 10. Reader unit 10 comprises a sensor 11 which is suitable for sensing a signal transmitted by the transmission means 9 of device 8. In addition reader unit 10 comprises transmission means 12 which are suitable for transmitting a signal which is discernible by the user 2, such as a signal transmitted by transmission means 6 of device 5 of fig. 2.

The transmission means 9 of device 8 of fig. 3 may be of a type which transmits a signal which is undiscernible by user 2. Reader unit 10 may be used to convert a signal transmitted by transmission means 9 into a transmission signal which is discernible by user 2. Yet, the example of fig. 3 is also applicable for a case in which a signal transmitted by transmission means 9 is discernible by user 2, but which is possibly difficult to discern. For example, the signal transmitted by transmission means 9 may consist of a series of light flashes with short intervals, while transmission means 12 may provide a converted presentation of a passkey carried by the light flashes, such as a spoken or readable message.

The method exemplified by fig. 4 differs from the method shown by fig. 3 in that Bluetooth device 1 is replaced by a Bluetooth device 15, which comprises a sensor means 16 instead of the input means 4 of device 1, and reader unit 10 is replaced by a reader unit 18 having sensor means 19 and transmission means 20.

Reader unit 18 differs from reader unit 10 of fig. 3 basically in that a signal carrying a passkey transmitted by transmission means 20 need not to be discernible by user 2 but must be suitable to be sensed by sensor means 16 of device 15.

Preferably, sensor means 16 consist of means which are already present for normal operation of device 15.

The method exemplified by fig. 5 differs from the method shown by fig. 4 in that Bluetooth device 15 is replaced by Bluetooth device 22 having sensor means 23 which are suitable for sensing a

signal carrying a passkey transmitted by transmission means 9 of device 8 directly. The user 2 only needs to bring devices 8 and 22 in proper proximity of each other.

As described herein before the method and system according to the invention and as exemplified with reference to figs. 2-5 make it possible for a manufacturer to only manufacture identical Bluetooth devices not containing passkeys and not having passkeys allocated thereto, while preserving the possibility of secure communications between two Bluetooth devices offered by Bluetooth technology, against very reduced costs.

C L A I M S

1. Method for bonding a first Bluetooth device (5, 8) to a second Bluetooth device (1, 15, 22) comprising:

a) placing the devices in a bonding mode;

b) providing a passkey which is identical for both devices;

c) storing the passkey in each device;

d) generating identical passkey based information in both devices;

e) leaving the bonding mode while further ignoring the password;

characterized in that:

the step of providing a passkey includes:

b1) generating a random passkey by the first device;

b2) presenting the random passkey by the first device to its outside by non-radio transmission;

b3) sensing the random passkey from the outside of the first device;

b4) providing the sensed passkey to the second device.

2. Method for bonding two Bluetooth devices (1, 5) according to claim 1, characterized in that the sensing of the passkey and providing the sensed passkey to the second device (1) are carried out by a user (2) of the devices (1, 5) only.

3. Method for bonding two Bluetooth devices (1, 8) according to claim 1, characterized in that the sensing of the passkey is carried out by a reader unit (10) which is separate from the first device (8), the reader unit presents the sensed passkey to its outside by non-radio transmission and discernable to a user of the devices, and the passkey discerned from the reader unit by the user (2) is entered by the user into the second device (1).

4. Method for bonding two Bluetooth devices (8, 15) according to claim 1, characterized in that the sensing of the passkey is carried out by a reader unit (18) which is separate from the first device (8) and the reader unit presents the sensed passkey to its outside by non-radio transmission and discernable to a sensor (16) of the

second device (15) to thereby provide the second device with the passkey.

5. Method for bonding two Bluetooth devices (8, 22) according to claim 1, characterized in that the sensing of the passkey is carried out by a sensor (23) of the second device (22) to provide the second device with the passkey.

6. System of a first Bluetooth device (5, 8) and a second Bluetooth device (1, 15, 22), the devices comprising:

a) mode selection means for placing the devices in a bonding mode;

b) means for providing a passkey to the devices, the passkey being identical for both devices;

c) storage means for storing the respective passkey in each device;

d) generator means for generating identical passkey based information;

e) reset means for leaving the bonding mode and for clearing the passkey;

characterized in that:

the means for providing the passkey includes:

b1) generator means of the first device for generating a random passkey;

b2) output means (6, 9) of the first device for outputting the random passkey by non-radio transmission.

7. System according to claim 8, characterized in that the output means (6) of the first device (5) outputs the passkey in a manner which makes it discernible by a user (2) of the devices (1, 5).

8. System according to claim 8, characterized by a reader unit (10) having sensor means (11) for sensing the passkey outputted by the output means (9) of the first device (8) and having output means (12) for outputting the sensed passkey by non-radio transmission and discernable to a user (2) of the devices (1, 8).

9. System according to claim 8, characterized by a reader unit (18) having sensor means (19) for sensing the passkey outputted by the output means (9) of the first device (8) and having output means (20) for outputting the sensed passkey by non-radio transmission and discernable to sensor means (16) of the second device (15) to thereby provide the second device with the passkey.

10. System according to claim 8, characterized in that the output means (9) of the first device (8) outputs the passkey in a manner which makes it discernable to sensor means (23) of the second device (22) to thereby provide the second device with the passkey.

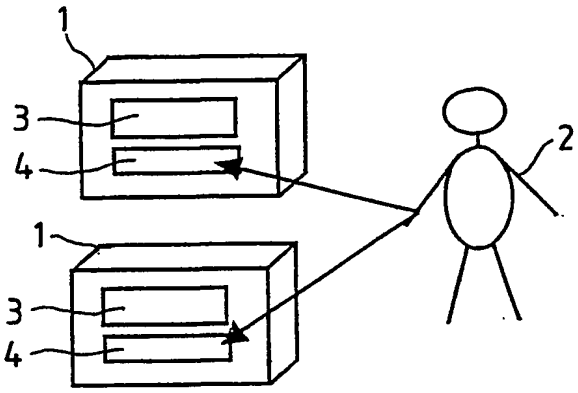


Fig 1 (PRIOR ART)

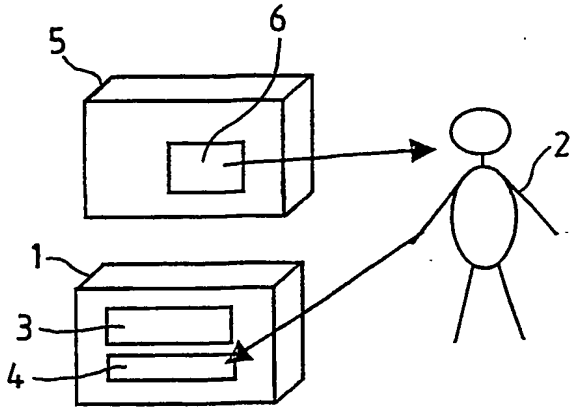


Fig 2

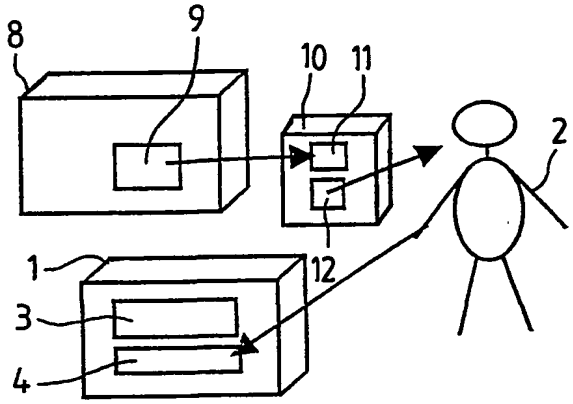


Fig 3

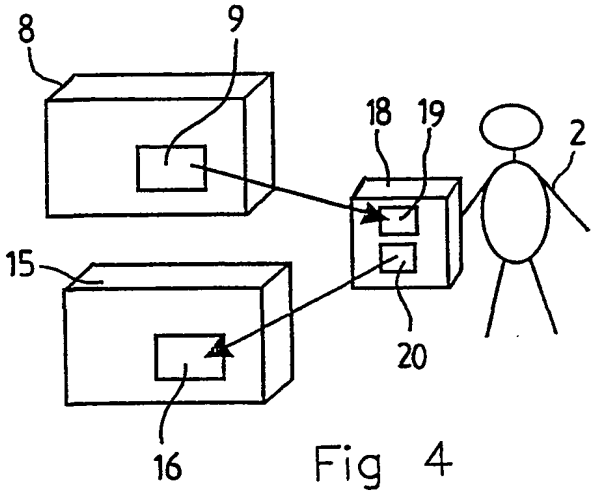


Fig 4

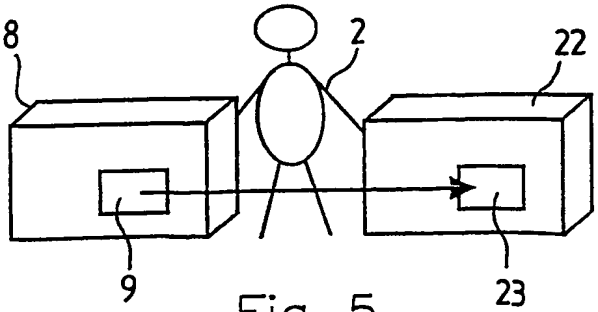


Fig 5

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 1 024 626 A (IBM) 2 August 2000 (2000-08-02) column 6, line 15 -column 7, line 40; figure 1 column 10, line 25 - line 50 column 13, line 5 - line 35	1-10
A	DE 199 24 232 A (GIESECKE & DEVRIENT GMBH) 7 December 2000 (2000-12-07) abstract; figure 1	2,3,7,8
A	WO 97 36422 A (BATCHELOR STEVE ;INTEL CORP (US); PERRY BURT (US)) 2 October 1997 (1997-10-02) page 2; figure 1	4,9

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
28 August 2001	10/09/2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Carnerero Álvaro, F

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
T	THE BLUETOOTH FORUM: "Generic Access Profile" BLUETOOTH SPECIFICATION VERSION 1.1, 'Online! 22 February 2001 (2001-02-22), XP002175814 Retrieved from the Internet: <URL:http://www.bluetooth.com/developer/specification/BLUETOOTH_11_Profiles_Book.pdf > 'retrieved on 2001-08-24! cited in the application page 29 page 43 -page 45 page 53	1-10

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1024626 A	02-08-2000	CN 1262563 A	09-08-2000
		JP 2000224156 A	11-08-2000
DE 19924232 A	07-12-2000	AU 5809800 A	18-12-2000
		WO 0074003 A	07-12-2000
WO 9736422 A	02-10-1997	US 6195501 B	27-02-2001
		AU 2321097 A	17-10-1997
		CA 2250925 A	02-10-1997
		EP 0890260 A	13-01-1999